DEPARTMENT OF THE NAVY
NAVAL HEALTH RESEARCH CENTER
POST OFFICE BOX 85122
SAN DIEGO, CA 92186-5122

IN REPLY REFER TO:
NAVHLTHRSCHCENNOTE 6500.1
00B
25 Jan 07

NAVHLTHRSCHCEN NOTICE 6500

Subj: PROTECTION OF HEALTH INFORMATION IN RESEARCH

Ref: (a) DoD 6025.18-R, "DoD Health Information Privacy Regulations," January 24, 2003
(b) Code of Federal Regulations, 45 CFR § 164.530, "Privacy of Individually Identifiable Health Information, Administrative Requirements," December 28, 2000

Encl: (1) Naval Health Research Center Policies and Procedures for Protecting Personal Health Information in Research
(2) Naval Health Research Center Research Notice of Privacy Practices

1. Purpose. To establish and disseminate policies and procedures for the protection of individually identifiable health information in the conduct of research at the Naval Health Research Center and its subordinate laboratories.

2. Discussion. Reference (a) requiresall Department of Defense covered entities to adopt written policies and procedures for protecting private health information. Reference (b) indicates that the policies and procedures are to be reasonably designed to ensure compliance, taking into account the size of and the types of activities that relate to protected health information undertaken by the covered entity. Enclosure (1) are procedures to be followed by Naval Health Research Center to minimize the likelihood of unauthorized disclosures of protected health information. Enclosure (2) is a summarized 'Notice of Privacy Practices' at Naval Health Research Center to be given to any research participant upon request.

3. Responsibilities. All members of the command are responsible for familiarizing themselves and adhering to the policies set forth in this Notice.

4. Action. Enclosures (1) and (2) are adopted by signature below.

K. R. THOMPSON
Acting

Distribution:
All hands

NAVHLTHRSCHCEN NOTICE 6500 25 January 2007

PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH

Policies and Procedures for Implementation of the Privacy Rule in Research

Naval Health Research Center
P.O. Box 85122
San Diego, CA 92186-5122

PROTECTING PERSONAL HEALTH INFORMATION IN RESEARCH

Policies and Procedures for Implementation of the Privacy Rule in Research

Naval Health Research Center
P.O. Box 85122
San Diego, CA 92186-5122

TABLE OF CONTENTS

Section 1 Background

The purpose of this document is to delineate the policies and procedures to which the Naval Health Research Center will adhere with regard to implementation and enforcement of the federal Health Insurance Portability and Accountability (HIPAA) Privacy Rule.

Health Insurance Portability and Accountability Act

In August 1996, the Health Insurance Portability and Accountability Act was signed into law. The Act included provisions for health insurance portability, fraud control, tax related provisions, group health plan requirements, revenue offset provisions, and administrative simplification requirements. All health plans, health care clearinghouses, and health care providers who conduct certain administrative transactions electronically must comply with HIPAA. The Military Health System, of which the Navy Bureau of Medicine and Surgery (BUMED) is a component, qualifies as a health plan that must comply with HIPAA regulations. The Naval Health Research Center and its detachments, as part of the BUMED organization, have been designated "covered entities" for HIPAA compliance purposes.

One element of HIPAA is the Privacy Rule. The Privacy Rule establishes minimum federal standards for the use and disclosure of protected health information (PHI). PHI is individually identifiable health information, including demographics, transmitted or maintained in any form or medium. The Privacy Rule confers certain rights on individuals, including the rights to access and amend their health information and the right to obtain a record of when and why their PHI has been shared with others. The Privacy Rule also establishes conditions under which covered entities may disclose PHI to others. Covered entities and individuals that fail to comply with the Privacy Rule are subject to civil and criminal penalties. Compliance with the Privacy Rule was required as of April 14, 2003.

DoD Health Information Privacy Regulation

The Department of Defense (DoD) issued DoD 6025.18-R, "DoD Health Information Privacy Regulation" 24 January 2003 to prescribe permissible uses and disclosures of PHI. Compliance with DoD 6025.18-R is mandatory for all DoD Components.

Definitions

Accounting for Disclosures - Covered entities must maintain an accounting of all disclosures of PHI other than 1) for treatment, payment, and health care operations; 2) disclosures made with Authorization from the individual whose PHI is being disclosed; and 3) certain other limited disclosures. For disclosures that need to be in the accounting, the accounting must include all disclosures that have been made in the previous 6 years. However, PHI disclosures made before April 14, 2003 are not part of the accounting requirement.

Authorization - An individual's written permission to allow a covered entity to use or disclose specified PHI for a particular purpose. Except as otherwise permitted by the Privacy Rule, a covered entity may not use or disclose PHI for research purposes without a valid Authorization.

Business Associate - A person or entity who, on behalf of a covered entity, performs or assists in a function involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing, and quality assurance reviews. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

Covered Entity - A (1) health plan, (2) health care clearinghouse, or (3) health care provider who transmits health information in electronic form in connection with a HIPAA transaction.

Disclosure - The release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

Health Information - Any information, whether oral or recorded in any form or medium, that (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school, or health care clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individual - The person who is the subject of protected health information.

Individually Identifiable Health Information - Information that (1) is created or received by a covered entity; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) is accompanied by information (a) that identifies the individual; or (b) with which there is a reasonable basis to believe can be used to identify the individual.

Limited Data Set - Refers to health information that excludes 16 categories of direct identifiers and which may be used or disclosed without obtaining either an individual's Authorization or a formal waiver so long as a data use agreement is executed before that data is disclosed.

Minimum Necessary – Refers to the least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request for protected health information. Unless an exception applies, this standard applies to a covered entity when using or disclosing PHI or when requesting PHI from another covered entity. A covered entity that is using or disclosing PHI for research without the individual's Authorization must make reasonable efforts to limit PHI to the minimum necessary.

Protected Health Information – PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Research - A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Use - With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within the covered entity that maintains such information.

Waiver or Alteration of Authorization - The documentation that an IRB or Privacy Board has waived all or portions of the Privacy Rule's requirement that an individual must authorize a covered entity to use or disclose that individual's PHI before it can be used or disclosed.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity.

Section 2 - Responsibilities of NHRC as a Covered Entity

While NHRC does not provide health care, NHRC is considered a "covered entity," and as such must comply with the HIPAA Privacy Rule. NHRC's responsibilities include:

- Adopting clear privacy policies and procedures;
- Designating a HIPAA Privacy official responsible for seeing that privacy procedures are adopted and followed, and who will also receive and handle complaints;
- Training members of its workforce on the policies and procedures for safeguarding protected health information as are necessary and appropriate for those workforce members to carry out their functions within NHRC;
- Ensuring that information is provided to research participants about their privacy rights and how their information can be used;
- Providing a Notice of Privacy Practices to research participants upon request;
- Responding to research participant's queries regarding rights provided by the Privacy Rule;
- Enacting safeguards to ensure that research participant's PHI are available only to those research staff and associates authorized to access that medical data; and

- Maintaining the required administrative documentation demonstrating compliance with the Privacy Rule.

NHRC will continuously evaluate and refine its HIPAA-related policies as needed to assure compliance with the Privacy Rule and any changes to it that may be adopted.

Other Federal Laws and Regulations Relating to Privacy Protections

Research conducted at NHRC is governed by 10 USC § 980, 32 CFR § 219, and other DoD, Navy, and local instructions. Although these human subject regulatory requirements include protections to help ensure the privacy of subjects and the confidentiality of information, the intent of the Privacy Rule, among other things, is to supplement these protections by requiring covered entities to implement specific measures to safeguard the privacy of individually identifiable health information. The Privacy Rule does not replace or act in lieu of these human subject protection regulations. Therefore, NHRC researchers are responsible for complying with the Privacy Rule, as well all regulations pertaining to the Protection of Human Subjects.

State Law

As a general rule, state laws pertaining to healthcare are not applicable to healthcare programs and activities of the DoD. However, there are some matters for which DoD rules and procedures call for compliance with state law. For example, in cases involving disclosure of PHI about a minor to a parent, guardian, or person acting in loco parentis, the state law where the treatment is provided shall be applied. In any other case in which there is a conflict between the DoD Regulation and state law, the DoD Regulation shall apply, unless DoD rules, procedures, or other applicable policy specifically call for the DoD Components to follow state law with respect to the matter at issue.

Section 3 - Use and Disclosure of PHI for Research Purposes

In the course of conducting research, NHRC researchers may have reason to want to obtain, create, use, and/or disclose individually identifiable health information. For example, Protected Health Information (PHI) may be created in the conduct of physiological performance trials or through the administration of surveys, and existing PHI may be used in epidemiologic research that accesses DoD databases of inpatient and outpatient visits. Under the Privacy Rule, NHRC researchers are permitted to use and disclose PHI for research with the individual authorization of the research participant, or without individual authorization under the limited circumstances set forth in the Privacy Rule (45 CFR §§ 164.508, 164.512(i)).

Authorization for Research Use and Disclosure

The Privacy Rule permits NHRC researchers to use or disclose PHI for research purposes when a research participant authorizes the use or disclosure of information about him or herself. The written Authorization focuses on privacy risks and states how, why, and to whom the PHI will be used or disclosed. This Authorization is in addition to informed consent to participate in research but may be combined with the informed consent document.

NHRC researchers must obtain written Authorization signed by the research participant for uses and disclosures of PHI, and the purpose of that PHI usage must be clearly delineated in that Authorization. The Authorization must pertain to a specific research study, and not to nonspecific research or to future projects of a unspecific nature. An individual may authorize their PHI to be entered into a research repository or database, but that authorization should be conditioned on future IRB or Privacy Board review of any proposed uses or disclosures to determine whether re-Authorization is needed.

1. Core Elements and Requirements

An Authorization must contain the following specific elements and meet the stated requirements, per 45 CFR § 164.508(c):

A. Elements.

i. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

ii. A description of each purpose of the requested use or disclosure;

iii. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

iv. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

v. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;

vi. A statement that the covered entity will not condition treatment or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;

vii. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;

viii. A statement that the individual may:

a. Inspect or copy the protected health information to be used or disclosed; and

b. Refuse to sign the authorization.

ix. If applicable, a statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule; and

x. Signature of the individual and the date;

B. Plain language requirement. The authorization must be written in plain language.

C. Copy to the individual. A covered entity must provide the individual with a copy of the signed authorization

The NHRC IRB Informed Consent template contains language that illustrates the inclusion of the elements and required statements. A signed copy must be provided to the research participant.

2. Waiver or Alteration of the Authorization Requirement

To use or disclose PHI without the authorization of the research participant who is the subject of the health information, NHRC researchers must obtain one of the following:

- Documentation that an Institutional Review Board (IRB) or Privacy Board has approved an alteration to or waiver of authorization (45 CFR § 164.512(i)(1)(i));

- Documentation from the IRB accepting the PI's representation that the use is necessary to prepare a research protocol or for similar purposes preparatory to research (45 CFR § 164.512(i)(1)(ii)); or

- Documentation from the IRB accepting the PI's representation that the use or disclosure is solely for research on PHI of decedents. (45 CFR § 164.512(i)(1)(iii)).

A. Criteria for IRB Approval of Authorization Waiver

NHRC researchers may use or disclose protected health information without the written consent or authorization of the research participant if the NHRC IRB approves a waiver or alteration of the Authorization requirement. The following criteria must be satisfied for the NHRC IRB to approve a waiver of authorization under the Privacy Rule:

A) The use or disclosure of protected health information involves no more than minimal risk to the individuals;

(B) The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;

(C) The research could not practicably be conducted without the alteration or waiver;

(D) The research could not practicably be conducted without access to and use of the protected health information;

(E) The privacy risks to individuals whose protected health information is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the individuals, and to the importance of the knowledge that may reasonably be expected to result from the research;

(F) There is an adequate plan to protect the identifiers from improper use and disclosure;

(G) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(H) There are adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart.

IRB documentation of the waiver or alteration of Authorization must include:

(A) Identification and date of action. A statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;

(B) Waiver criteria. A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization satisfies the criteria listed above to approve a waiver;

(C) Protected health information needed. A brief description of the protected health information for which use or access has been determined by the IRB to be necessary;

(D) Review and approval procedures. A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and,

(E) Required signature. The documentation of the waiver of authorization must be signed by the IRB/Privacy Board chair, or other member as designated by the chair.

B. Reviews Preparatory to Research

Investigators may use PHI without authorization or waiver to prepare a research protocol, or for a similar purpose preparatory to research if the following written representations are made by the investigator and provided to and accepted in writing by the NHRC IRB:

A. Use or disclosure is solely for purposes of reviewing the PHI as necessary to prepare a research protocol or for similar purposes preparatory to research (e.g., to design a study or to assess the feasibility of conducting a study).

B. The PHI being sought to be used is limited to the minimum necessary to achieve the purpose(s) of the review.

C. The PHI for which use or access is sought is necessary for the research purposes.

D. No PHI will be removed from the covered entity by the researcher in the course of the research review.

Researchers should note that any preparatory research activities involving human subjects research must be reviewed and approved by the NHRC IRB and must satisfy any informed consent requirements unless waived by the IRB.

C. Research on Decedent's Information

To use or disclose PHI of deceased individuals for research, NHRC is not required to obtain Authorizations from the personal representative or next of kin. However, NHRC must obtain from the researcher who is seeking access to decedents' PHI:

A. Representation that the use or disclosure is sought is solely for research on the PHI of decedents;

B. Representation that the PHI for which use or disclosure is sought is necessary for the research purposes; and,

C. Documentation, at the request of NHRC, of the death of the individuals about whom information is being sought.

3. Limited Data Sets with a Data Use Agreement

The Privacy Rule (45 CFR § 164.514) permits use and disclosure of PHI in a limited data set without obtaining an Authorization or a waiver of Authorization. NHRC may use or disclose a limited data set for research activities if the disclosing entity and the limited data set recipient enter into a data use agreement. Limited data sets may be used or disclosed only for purposes of research, public health, or health care operations. Because limited data sets may contain potentially identifiable information, they are still PHI.

A limited data set is described as health information that excludes certain, listed direct identifiers but that may include indirect identifiers such as treatment date. The direct identifiers listed in the Privacy Rule's limited data set provisions apply both to information about the individual and to information about the individual's relatives, employers, or household members. The following variables must be removed from health information if the data are to qualify as a limited data set:

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code.
3. Telephone numbers.
4. Fax numbers.
5. Electronic mail addresses.
6. Social security numbers.
7. Medical record numbers and voiceprints.
8. Health plan beneficiary numbers.
9. Account numbers.
10. Certificate/license numbers.
11. Vehicle identifiers and serial numbers, including license plate numbers.
12. Device identifiers and serial numbers.
13. Web universal resource locators (URLs).
14. Internet protocol (IP) address numbers.
15. Biometric identifiers, including fingerprints
16. Full-face photographic images and any comparable images.

A data use agreement is the means by which NHRC obtains satisfactory assurance that the recipient of the limited data set will use or disclose the PHI in the data set only for specified purposes.

A data use agreement for a limited data set must:

A. Establish the specific permitted uses and disclosures of the limited data set by the recipient, consistent with the purpose of the research, and which may not include any use or disclosure that would violate the Privacy Rule if done by the entity providing the data;

B. Identify and limit who can use or receive the limited data set; and

C. Require the recipient to agree to the following:

i. Not use or disclose the information other than permitted by the data use agreement or otherwise required by law;

ii. Use appropriate safeguards to prevent the use or further disclosure of the information;

iii. Report to NHRC any uses or disclosures in violation of the agreement of which the recipient becomes aware;

iv. Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same standards, restrictions, and conditions stated in the data use agreement with respect to the limited data set; and

v. Not attempt to identify the information or contact the individuals.

If a covered entity is the recipient of a limited data set and violates the data use agreement, it is deemed to have violated the Privacy Rule. If the covered entity providing the limited data set knows of a pattern of activity or practice by the recipient that constitutes a material breach or violation of the data use agreement, the covered entity must take reasonable steps to correct the inappropriate activity or practice. If the steps are not successful, the covered entity must discontinue disclosure of PHI to the recipient and notify the appropriate parties.

4. Providing PHI data sets to Business Associates

The Privacy Rule also protects individually identifiable health information when it is created by or provided to a business associate. A "business associate" is a person or entity conducting certain functions on behalf of a covered entity. The Rule's business associate provisions can be found in Rule 45 CFR § § 164.502(e), 164.504(e). Before NHRC discloses PHI to a business associate, NHRC must obtain satisfactory assurances, in the form of a written agreement, that the business associate will appropriately safeguard the information. When the agreement is between two governmental entities it shall be labeled as a Memorandum of Understanding, and when it is between NHRC and a private entity, it shall be labeled as a Business Associate Agreement.

An agreement between the covered entity and a business associate must:

(i) Establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate HIPAA requirements if done by the covered entity;

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

(D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information to the subject of that PHI;

(F) Make available protected health information for amendment, and incorporate any amendments to protected health information;

(G) Make available the information required to provide an accounting of disclosures;

(H) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the covered entity available to the Secretary of Health and Human Services for purposes of determining the covered entity's compliance with this subpart; and

(I) At termination of the contract, if feasible, return or destroy all protected health information received from the covered entity that the business associate still maintains in any form and retain no copies of such information, or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

5. Other Uses and Disclosures of PHI

Additional PHI uses and disclosures permitted under the Privacy Rule at 45 CFR § 164.512 without Authorization, waiver of Authorization, or data use agreement are summarized below. NHRC researchers seeking to use and disclose PHI for these or other purposes permitted under Section 164.512 should consult the Privacy Rule and NHRC's HIPAA Privacy Officer for further guidance.

Among other limited purposes, NHRC may disclose PHI without an Authorization, as follows:

A. To health oversight agencies for oversight activities authorized by law that are necessary for the appropriate oversight of government-regulated programs. For example, because Office for Human Research Protections (OHRP) is a health oversight agency under the Privacy Rule, NHRC may disclose PHI, without Authorization, to OHRP for purposes of determining compliance with the Protection of Human Subjects Regulations.

B. To the FDA with respect to an FDA-regulated product or activity for which that person has responsibility, for purposes related to the quality, safety, or effectiveness of the FDA-regulated product. For example, a covered entity may disclose adverse event/safety reports to sponsors of investigational new drugs.

C. To a public health authority that is authorized by law to collect or receive the information for purposes of preventing or controlling disease, injury, or disability. Activities included here are reporting disease, injury, and vital events, such as births and deaths, as well as conducting public health surveillance and interventions.

D. To a law enforcement official for a law enforcement purpose if in compliance with 1) a court order, or a subpoena or summons issued by a judicial officer; 2) a grand jury subpoena; or 3) a relevant and legitimate law enforcement inquiry where the requested information is specific and limited in scope and de-identified information could not reasonably be used.

All PHI disclosures made without the authorization of the individuals whose health information is being disclosed must be accounted for in writing. Thus, disclosures should only be made with the written acknowledgement of the HIPAA Privacy Officer.

NHRC workforce members must be aware that oral or written communications pose some risk of incidental disclosure of PHI. Workforce members must take responsibility for maintaining confidentiality when engaging in activities such as face-to-face discussions or telephone discussions of a research participant's medical condition or when reviewing lab tests or research findings.

6. "Minimum Necessary" Requirement

NHRC is required by 45 CFR § 164.514(d) to implement procedures that limit the PHI used, disclosed, or requested to the minimum amount reasonably necessary to achieve the purposes for which disclosure is sought. NHRC policies and procedures apply to researchers who are members of the NHRC's workforce and to any business associates. For all uses, disclosures and requests for PHI, the NHRC IRB, IRB Chairperson, or HIPAA Privacy Officer will examine the researcher's submitted documentation to review the persons indicated to need access to PHI and the specific PHI that is indicated as needed, as well as any other proposed conditions governing

such access. It is incumbent upon the researcher or other staff member seeking to use or disclose PHI to justify that the specific health information being used or disclosed is indeed the minimum needed to carry out the stated purpose.

Documentation of IRB or Privacy Board approval may be relied upon as establishing that the request for use or disclosure of protected health information meets the "minimum necessary" requirements.

7. Accounting for Research Disclosures (45 CFR § 164.528(a)(b))

NHRC must maintain an accounting of PHI disclosures made without the research participant's authorization (except for disclosures of a limited data set). Upon request, NHRC must provide the participant an accounting of each disclosure of that participant's PHI for the six years prior to the participant's request for an accounting, and must include the date of disclosure, identification of the entity who received the data, a description of the PHI disclosed, and a statement of the purpose of the disclosure. Where records of 50 or more individuals are disclosed for research purposes, the accounting must include the name of the research protocol, a description of the research that includes the purpose and criteria for selecting records, a description of the PHI disclosed, the dates of disclosures, the name, address, and phone number of the entity to whom the PHI was disclosed, and a statement that the PHI of the individual may or may not have been disclosed if disclosure of that individual's information cannot be specifically ascertained.

Research disclosures made pursuant to the research participant's authorization and disclosures of a limited data set to researchers with a data use agreement complying with 45 CFR § 164.514(e) are exempt from this accounting requirement.

8. De-Identified Data (45 CFR § 164.514)

Health information that is de-identified according to specific standards is not consider PHI, and as such, is not protected by the Privacy Rule. De-identified health information can be used and disclosed by an NHRC researcher without the Authorization of the subject of that data. NHRC may determine that health information is not individually identifiable in either of the two following ways.

A. Removing Identifiers

NHRC researchers may de-identify data by removing all 18 elements that could be used to identify the research participant or the participant's relatives, employers, or household members. The NHRC researcher also must have no actual knowledge that the remaining information could be used alone or in combination with other information to identify any research participant. Under this method, the identifiers that must be removed are all of the following:

1. Names. 2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census: a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people. b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000. 3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.	4. Telephone numbers. 5. Facsimile numbers. 6. Electronic mail addresses. 7. Social security numbers. 8. Medical record numbers. 9. Health plan beneficiary numbers. 10. Account numbers. 11. Certificate/license numbers. 12. Vehicle identifiers and serial numbers, including license plate numbers. 13. Device identifiers and serial numbers. 14. Web universal resource locators (URLs). 15. Internet protocol (IP) address numbers. 16. Biometric identifiers, including fingerprints and voiceprints. 17. Full-face photographic images and any comparable images. 18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification.

Under this method, a code or other means of record identification may be assigned and retained if that code is not derived from or related to the information about the research participant and could not be translated to identify the participant. NHRC may not use or disclose the code or other means of record identification for any other purpose and may not disclose its method of re-identifying the information. For example, a randomly assigned code that permits re-identification through a secured key to that code would not make the information PHI, because a random code would not be derived from or related to information about the individual and because the key to that code is secure.

B. Statistical Methods

NHRC researchers may also use statistical methods to establish de-identification instead of removing all 18 identifiers. Statistical de-identification must be certified by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable" and state that there is a "very small" risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in combination with other reasonably available information. The person certifying the de-identification must document the methods used as well as the result of the analysis that justifies the determination. NHRC is required to retain such certification, in written or electronic format, for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

9. Sanctions for noncompliance

Appropriate sanctions shall be applied against members of a workforce who fail to comply with the privacy policies and procedures outlined in this document or who are otherwise in violation of the HIPAA Privacy rule. Sanctions for noncompliance shall include, but not be limited to, additional data privacy safeguards applied to the staff member's research protocols, further privacy/security training as appropriate, loss of Principal Investigator privileges, loss of all research privileges, denial of access to protected health information, and/or suspension or loss of employment. The procedures outlined in NHRC's policies and procedures for handling allegations of scientific misconduct shall also be applicable to allegations of noncompliance with Privacy Rule regulations. HIPAA regulations allow for federal civil and criminal penalties to be applied in addition to any local sanctions where the violation warrants such penalties.

Section 4 - Research Participant's Rights

In addition to establishing conditions for the use and disclosure of Protected Health Information (PHI), the Privacy Rule establishes certain rights of individuals with respect to their health information. Individuals have the right to:

- Be told how their data will be used, to whom it will be disclosed and any data privacy and confidentiality safeguards;
- Inspect or request amendment to PHI provided to NHRC;
- Revoke their Authorization for NHRC to further use the individual's PHI;
- Request and receive a written accounting from NHRC of when and why their PHI has been disclosed;
- Register a complaint if they believe a violation of the Privacy Rule has occurred;
- Be provided a Notice of Privacy Practices upon request.

Right to Know How PHI Will Be Used

NHRC researchers must inform individuals who provide PHI for research purposes about how that data will be used and/or disclosed, to whom it might be disclosed, how long that data will be maintained, and any data protection measures that will be implemented. In most instances where PHI is involved, research subjects will be informed of the above information in the informed consent document that explains the research, its purpose, the voluntary nature of the research, and any risks and benefits of the research.

Right to Inspect One's Own PHI

With few exceptions, NHRC researchers must allow individuals access to inspect and copy their medical records and other types of protected health information for as long as the information is maintained. Records containing PHI that research subjects might request to inspect could include surveys administered, medical charts, study eligibility questionnaires, records of adverse events, and records of physiologic measures that reflect on the individual's health status.

Information as to how to request access to their PHI should be provided in the informed consent form, or, where appropriate, in a separate PHI Use Authorization. Individuals requesting access to their research information at NHRC should be informed to make a written request directly to the investigator responsible for the study. The investigator would then provide the individual with convenient times and location for inspecting or obtaining a copy of the information, or, once the identity of the requestor is verified, arrange to have the requested information mailed to the requesting individual.

If NHRC denies access to an individual's own PHI, NHRC must provide a written denial to the individual, and the written denial must be in plain language, state the basis for denial, provide a description of how the individual may file a complaint, and provide the name and telephone number of the local Privacy Officer designated to receive complaints.

Right to Amend PHI

Individuals have the right to request amendment of any PHI maintained at NHRC if they have reason to believe the PHI contains inaccuracies. Individuals requesting an amendment to their research information at NHRC should contact the investigator responsible for the study.

NHRC must act on the individual's request for an amendment no later than 60 days after receipt of such a request by either making the amendment or by denying the request in writing. If NHRC is unable to act on the amendment within 60 days, a one-time delay of no more than 30 days is permitted by providing (within the initial 60 days) the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed. If NHRC accepts the amendment in whole or in part, NHRC must inform the individual in a timely manner that the amendment has been made. NHRC may deny an individual's request for amendment if it determines that the record that is the subject of the request is accurate and complete without amendment. If NHRC denies the request for amendment, NHRC must provide in writing a written denial (in plain language) within the required time limits; a basis for the denial; a description of how the individual can submit a written statement disagreeing with the denial, including the basis for disagreement; a statement that the individual may request that NHRC provide the individual's request for amendment and the written denial with any future disclosure of the PHI; and a description of how the individual can file a complaint, including the title, name, and contact number of the Privacy Officer. Even if NHRC denies the request for an amendment, NHRC must link or append all

relevant, written documents pertaining to the request to the PHI that was requested to be amended.

Right to Request Restrictions on Use and Disclosure of PHI

Individuals have the right to request restrictions on how NHRC uses and discloses their PHI. NHRC is not required to agree to the restriction, but should honor all reasonable requests that involve data privacy or social stigma. If NHRC does agree, it must honor the agreed-to-restrictions unless they are subsequently revoked by the individual, or unless the individual is in need of emergency medical treatment.

Right to Revoke Authorization for the Use or Disclosure of PHI

Individuals have the right to revoke their Authorization for further uses and disclosure of their PHI. Individuals wishing to revoke their Authorization must submit a written request to the investigator responsible for the study. If the PHI has already been used to perform an analysis or other evaluation for the study, the results of those analyses can be retained. NHRC researchers may continue to use the individual's PHI as necessary to account for the subject's withdrawal from the study or to report adverse events. However, the researcher may not continue to use or disclose for research purposes any PHI previously collected or extracted after the individual revokes the authorization, nor may additional PHI of that individual be collected after that time. NHRC researchers must inform any other individuals or sites involved in the research of the individual's revocation of authorization.

Right to Receive an Accounting of PHI Disclosures

Upon request, NHRC must provide individuals a written record of any disclosures of their PHI that were made pursuant to a waiver of Authorization within the previous six years. This is known as an accounting of disclosures. It is important to emphasize the difference between a use and a disclosure of PHI. In general, the use of PHI means communicating that information within the covered entity. A disclosure of PHI means communicating that information to a person or entity outside NHRC. The Privacy Rule restricts both uses and disclosures of PHI, but it requires an accounting only for PHI disclosures. The right to an accounting also applies to disclosures of decedents' information and disclosures preparatory to research. Individuals requesting an accounting of disclosure of their PHI should be referred to the NHRC Privacy Officer. NHRC is not required to provide an accounting to the individual in the following situations: where the PHI was disclosed for treatment, payment, or health care operations; when there was a prior Authorization from the individual for the disclosure; where the PHI was disclosed as part of a limited data set; where disclosure was to a health oversight agency; or where disclosure was for national security or intelligence purposes.

Because all human subjects research protocols require IRB approval before the research may commence, the HIPAA Privacy Officer, who will generally be an IRB member, will be made aware of any proposed PHI disclosures before they are made. Disclosures of PHI will only be made after any required business associate agreements or memoranda of understanding are signed by both the entity disclosing

the data and the entity receiving the data. The HIPAA Privacy Officer will then document the disclosure, including the identity of the individuals who's PHI was disclosed, the dates of the disclosure, and the specific PHI disclosed. It is only through a complete accounting of all disclosures by NHRC staff that the HIPAA Privacy Officer can be prepared to respond to any queries received from individuals seeking to know if their PHI has been disclosed.

Right to File Complaints

Individuals have the right to complain to the covered entity and to the Secretary of Health and Human Services if they believe a violation of the Privacy Rule has occurred. Complaints to NHRC must be made in writing and should be directed to the Commanding Officer or the NHRC Privacy Officer. A complaint must name the person that is the subject of the complaint and describe the acts or omissions believed to be in violation of the HIPAA regulations. A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred. Individuals seeking to file a complaint shall be informed in writing of the above procedures for filing a complaint and shall be informed that they will not be retaliated against for filing a complaint. Complainants shall also be informed that they have the right to complain to the Secretary of Health and Human Services if they are unsatisfied with the response from NHRC but must do so within 180 days of when the complainant knew or should have known that the act or omission complained of occurred.

Right to a Notice of Privacy Practices

Research participants have the right, upon request, to a separate written notice of the privacy practices and the individual's rights with regard to protected health information. The Notice of Privacy Practices must delineate all the Research Participant's rights listed in this section, and how the participant may exercise these rights, including how to make contact with the HIPAA Privacy Officer to request further information.

Section 5 - Training

HIPAA regulations require that all workforce members of covered entities be trained about their responsibilities for maintaining the confidentiality of individual health information as necessary and appropriate to their workplace function. Federal regulations also require that HIPAA training be documented for accounting to the Department of Health and Human Services when requested.

Initial Education

All members of the NHRC workforce who potentially are exposed to protected health information, and supervisors of staff that come in contact with PHI, must successfully complete HIPAA training using the TRICARE Management Activity (TMA) online training system (MHS Learn) before gaining access to protected health

information. Courses will be assigned as necessary and appropriate for the workforce member to carry out their function at NHRC. Course assignments will typically be based on the member's job position and will, at a minimum, include the basics of HIPAA Privacy and Security.

Completion of other HIPAA training programs may be accepted in lieu of TMA training if the prior training is deemed equivalent by the HIPAA Privacy Officer to that received through MHS Learn.

Continuing Education

Per TRICARE Management Activity, NHRC workforce must also complete annual HIPAA Refresher Training. Refresher training should be completed through the HIPAA Refresher Courses available on the TMA training website.

Documentation of Training

Individuals are responsible for maintaining source documentation of their own initial and continuing education, and for providing written documentation of the completed training to NHRC IRB/HIPAA staff. IRB staff will then verify that each individual listed in a research protocol submitted for review has met the education requirement.

Section 6 - Damage Mitigation

In the event of an improper use or disclosure of PHI, Department of Health and Human Services (DHHS) expects that NHRC will demonstrate that policies and procedures have been implemented to minimize such a re-occurrence in the future, and that steps have been taken to mitigate the impact of the disclosure. To the extent practicable, NHRC will:

1. Contain the damage and stop further use or disclosure;

2. Utilize violations as a means to identify system lapses and to modify policies or procedures; and

3. Inform research subjects, where appropriate, of any improper use or disclosure arising from a violation of HIPAA regulations.

Section 7 - Documentation Requirements

The Privacy Rule requires NHRC to retain:

- NHRC's official written HIPAA Privacy Rule policies and procedures;
- Documentation of the identity of the individual who is responsible for the development and implementation of the policies and procedures at NHRC;
- Documentation of the identity of the individual and title of the person who is responsible for receiving and responding to HIPAA-related complaints;
- Business Associate Agreements and Memoranda of Understanding governing the sharing of protected health information (PHI) shared with outside entities;
- Authorizations of research participants allowing use or disclosure of their protected health information;
- Formal documentation from the IRB of any waivers of authorizations to use or disclose PHI;
- Written requests and responses to requests for access or copying of PHI by the individuals who provided that PHI;
- Written requests and responses to requests for amendment of PHI maintained at NHRC;
- Documentation of disclosures of PHI made without the specific authorization of the individual who's PHI was disclosed;
- Written requests for an accounting of PHI disclosures and responses to those requests for an accounting;
- Documentation of training received by members of the workforce on HIPAA policies and procedures;
- HIPAA-related complaints received and their disposition;
- Sanctions applied against members of the workforce who fail to comply with the privacy policies and procedures of NHRC;
- Documentation of the administrative, technical, and physical safeguards to protect the privacy of PHI.

Documentation shall be maintained in hard copy or electronic format for a minimum of six years.

NAVAL HEALTH RESEARCH CENTER

NOTICE OF PRIVACY PRACTICES

Effective Date: January 1, 2007

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED. PLEASE REVIEW IT CAREFULLY.

The Naval Health Research Center (NHRC), San Diego, California, is dedicated to adhering to a strict quality standard regarding the use and disclosure of your protected health information. This Notice of Privacy Practices is provided to you as a requirement of the Health Insurance Portability and Accountability Act (HIPAA). It describes how protected health information about you may be used and disclosed and your rights to access and amend this information.

WHO WILL FOLLOW THIS NOTICE

The practices described in this notice will be followed by anyone representing NHRC.

OUR DUTIES TO YOU REGARDING YOUR PROTECTED HEALTH INFORMATION

"Protected health information" is individually identifiable health information. This information includes personal identifiers when coupled with information relating to your past, present, or future physical or mental health, including your health status or any clinical test results that may be performed as part of your participation in a research study. NHRC is required by law to do the following:

- Make sure that your protected health information is kept private.
- Make available to you this notice of our legal duties and privacy practices related to the use and disclosure of your protected health information.
- Follow the terms of the notice currently in effect.
- Communicate any changes in the notice to you.

HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

We generally must have your written, signed authorization to use and disclose information about you. We may use and disclose information about you for any of the following reasons:

Participation in Research Studies. We may use and disclose health information about you when authorized by law, for example, if their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information. We may use information about you to provide you with research study related care and services. Our staff may need to know if you have health problems that could complicate your participation in or include/exclude you from participation in a research study. The investigator may discuss your information with another investigator for the purpose of making recommendations regarding your research study participation.

We may also use and disclose your protected health information to provide, coordinate, or manage medical treatment for any adverse experiences that you may experience during the research study. This may include the coordination or management of your health care with a third

party. For example, we may disclose your protected health information, as necessary, to a medical treatment facility or other health care provider who administers care to you. In emergencies, we will use and disclose your protected health information to provide the treatment you require.

Research Operations. We may use or disclose your information for research operations. For example, we may use your information to contact you to remind you of your appointment, to inform you about research related test results, or to clarify information you have provided.

Research Oversight. We may use and disclose information about you to organizations that sponsor our research, organizations that monitor our research, ethical review boards, and to the Food and Drug Administration (FDA) upon request. This information will be incorporated in the research study informed consent form, and in some instances, you may be asked to sign a separate HIPAA Authorization for this purpose.

SPECIAL SITUATIONS

We may use or disclose health information about you without your permission for the following purposes, subject to applicable legal requirements and limitations:

Required By Law. We will disclose health information about you when required to do so by federal, state or local law. If you are involved in any judicial or administrative proceedings, in response to a court order or administrative tribunal (if such a disclosure is expressly authorized). We may release health information if asked to do so by a law enforcement official in response to a court order, subpoena, warrant, summons or similar process, subject to applicable legal requirements. We may also disclose your protected health information to comply with workers' compensation laws and other similar legally established programs.

Military Activity and National Security. When the appropriate conditions apply, we may use or disclose protected health information of individuals who are Armed Forces personnel (1) for activities believed necessary by appropriate military command authorities to ensure the proper execution of the military mission including determination of fitness for duty; (2) for determination by the Department of Veterans Affairs (VA) for your eligibility for benefits; or (3) to a foreign military authority if you are a member of that foreign military service. We may also disclose your health information to authorized Federal officials for conducting national security and intelligence activities including protective services to the President or others.

Health or Safety Threats. We may use and disclose health information about you when necessary to prevent a serious threat to your health and safety or the health and safety of others. We may disclose health information about you for public health reasons in order to prevent or control disease, injury or disability; or report births, deaths, suspected abuse or neglect, non-accidental physical injuries, reactions to medications or problems with products. We may also disclose protected health information necessary for law enforcement authorities to identify or apprehend an individual.

Health Oversight Activities. We may disclose health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. These disclosures may be necessary to enable state and federal agencies to monitor the health care system, government benefit programs, other government regulatory programs, and to ensure compliance with civil rights laws.

Disclosures to Department of Defense (DoD) Health Plan. We may disclose health information if we are in possession of data that would normally be part of your DoD medical record but that has been lost or destroyed, and we are asked by appropriate medical personnel to provide information about prior medical conditions and treatments.

Information Not Personally Identifiable. We may use or disclose health information about you in a way that does not personally identify you or reveal who you are.

OTHER USES AND DISCLOSURES OF HEALTH INFORMATION

We will not use or disclose your information for any purpose other than those identified in the previous sections without your specific, written authorization. We must obtain your authorization separately or as part of a general or specific consenting process. If you give us authorization to use or disclose information about you, you may revoke that authorization in writing at any time. If you revoke your authorization, we will no longer use or disclose information about you, but we cannot take back any uses or disclosures already made during the time we had your permission.

YOUR RIGHTS REGARDING YOUR HEALTH INFORMATION

You have the following rights regarding health information we keep about you. You may exercise these rights by submitting a written request or electronic message to the NHRC Privacy Officer. Contact information for the Privacy Officer is on the last page of this Notice. Please be aware that your request may be denied; however, you may seek a review of the denial. Depending on your request, you may also have rights under the Privacy Act of 1974. The NHRC Privacy Officer can guide you in pursuing these options.

Right to Request Restrictions. You have the right to request a restriction or limitation on the health information we use or disclose about you. For example, you could ask that we not use or disclose information about a surgery you had. In your request, you must tell us (1) what information you want restricted; (2) whether you want to restrict our use, disclosure, or both; (3) to whom you want the restriction applied to, for example, disclosures to your spouse; and (4) an expiration date. You may revoke a previously agreed upon restriction, at any time, in writing. Restrictions are not transferable across research studies.

We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. If we do not approve your request, you may be ineligible to join a research study.

Right to Request Confidential Communications. You have the right to request that we communicate with you using certain means or at a certain location. For example, you can ask that we only contact you at work or by mail. Your request must specify how or where you wish to be contacted. We will not ask you the reason for your request. We will accommodate all reasonable requests, when possible.

Right to Inspect and Copy. You have the right to inspect and copy any health information that we have collected or extracted as part of our research studies, for as long as we maintain the information. If you request a copy of the information, we may charge a fee for the costs of retrieving, copying and mailing.

Right to Request Amendment. If you believe health information we have about you is incorrect or incomplete, you may ask us to amend the information as long as we maintain this information. While we accept requests for amendment, we are not required to agree to the amendment.

Right to an Accounting of Disclosures. You have the right to request an "accounting of disclosures." This is a list of the disclosures we have made of protected health information about you, that did not receive your prior consent, and which were not made for the purposes of treatment or health care operations. We may charge you for the costs of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. To obtain a paper copy, ask the principal investigator of the research study or the NHRC Privacy Officer.

CHANGES TO THIS NOTICE

We reserve the right to change this notice and to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. You are always entitled to a copy of the notice currently in effect.

COMPLAINTS

If you believe your privacy rights have been violated, you should first file a written complaint with the NHRC Privacy Officer. If the problem is not resolved at that level, you should contact the TMA Privacy Officer or the Department of Health and Human Services. No retaliation will occur against you for filing a complaint.

CONTACT INFORMATION

You may contact the NHRC Privacy Officer or the TMA Privacy Officer listed below for further information about the complaint process, or for further explanation of this document. For additional information regarding your privacy rights visit the TRICARE Web site at http://www.tricare.mil/tmaprivacy/Hipaa.cfm

NHRC Privacy Officer
Naval Health Research Center
P.O. Box 85122
San Diego, California, 92186-5122

By Phone: 1-619-553-8381
Email address: irb@nhrc.navy.mil

TMA Privacy Officer
TRICARE Management Activity
Information Management
Technology and Reenginnering Directorate
HIPAA Office
Five Skyline Place, Suite 810
5111 Leesburg Pike
Falls Church, VA 22041-3206

By Phone: 1-888-DOD-HIPA (1-888-363-4472)
Email address: hipaamail@tma.osd.mil